WHAT IS CLAIMED IS:

1. A wireless data network process, comprising the steps of:

providing a wireless local area network (WLAN) with a wireless access node, an internet connection and a mobile node (MN) with a wireless transceiver;

providing a serving GPRS support node with a radio network connection to a Gateway GPRS support packet gateway node (PGN) having a connection to the internet;

performing a key exchange between the MN and the PGN via radio waves, the GPRS support node and the connection to establish a shared secret key and to establish an IPsec Security Association (SA) between the MN and the PGN;

performing a hash of the key obtained at the PGN to obtain an authentication value for use in a Mobile IP protocol and using a security parameters index obtained from the SA as the Mobile IP for identifying the MN for authentication purposes;

performing a hash of the key obtained at the MN to obtain an authentication value for use in a Mobile IP protocol;

sending a Mobile IP registration request from the MN to a Home Agent (HA) hosted in the PGN using the authentication value established;

receiving the Mobile IP registration request at the PGN and authenticating the message using the authentication value and sending a Mobile IP registration reply to the MN.

2. A process according to claim 1, wherein said step of performing a key exchange includes performing a key exchange and subsequently using the Internet Key Exchange (IKE)

protocol with the MN requesting Encapsulated Security Protocol (ESP) for establishing the SA.

3. A process according to claim 2, further comprising:

receiving the Mobile IP registration reply at the MN and if the ESP established is not active, activating the ESP at the MN;

sending data packets from the MN to a target host on the internet using the ESP to the PGN with the PGN forwarding the packets to the target host;

replying by sending reply packets from the target host to the PGN with the PGN forwarding the reply packets using the ESP to the MN.

4. A process according to claim 3, further comprising:

establishing a connection of the MN on the Wireless LAN;

requesting a Mobile IP Care-Of-Address (COA) from Dynamic Host Configuration Protocol (DHCP) server on the Internet;

receiving the COA at the MN from across the Wireless LAN, wherein said step of sending data packets from the MN to a target host is via the wireless LAN connection to the internet and said step of replying by sending reply packets from the target host to the PGN is via the internet to the wireless LAN.

5. A process according to claim 4, further comprising:

terminating the connection with the PGN and detatching from the WLAN after the

conclusion of the data session to the MN 2.

6. A process according to claim 4, further comprising:

roaming with the MN into a region of the radio network and sending a message from the MN a Mobile IP registration request to the Home Agent hosted in the PGN indicating that the MN is on the home network and using the authentication value obtained within the message;

sending a Mobile IP registration reply from the PGN to the MN using the authentication value obtained.

7. A process according to claim 1, wherein said authentication value is a 128 bit authentication value.

8. A process according to claim 2, wherein the Mobile IP registration request can be sent via the established ESP.

9. A process according to claim 2, wherein the Mobile IP registration request is sent without the established ESP.

10. A wireless network system, comprising:

a mobile node with a wireless transceiver;

a serving GPRS support node (SGPRS);

a radio access network;

a gateway GPRS including a packet gateway node (PGN) with an internet connection, the PGN being capable of acting as a mobile IP home agent (HA);

a wireless local area network (WLAN) with a wireless access node and an internet connection;

at least one or both of a connection from the MN to the SGPRS and a connection between the MN and the WLAN;

keying established between the PGN and the MN using the MN to the SGPRS connection to form an IPSec Security Association between the MN and the PGN with a security parameters index obtained from the SA for identifying the MN;

a Mobile IP care-of-address obtained from a DHCP server through the connection between the MN and the WLAN;

an authentication value at the PGN for use in the IP mobile protocol formed by a MD-5 hash of the keying established between the PGN and the MN;

an authentication value at the MN for use in the IP mobile protocol formed by a MD-5 hash of the keying established between the PGN and the MN;

a Mobile IP registration based on a request message from the MN to the PGN with the HA hosted in the PGN using the authentication value established and with the PGN authenticating the message using the authentication value with a Mobile IP registration reply sent from the PGN to the MN.

11. A system according to claim 10, wherein said authentication value is a 128 bit authentication value.

12. A system according to claim 10, wherein said request message is sent from the MN to the PGN via the WLAN and a connection from the WLAN to the PGN over the internet.

13. A wireless network system, comprising:

a mobile node with a wireless transceiver;

a serving GPRS support node (SGPRS);

a radio access network;

a gateway GPRS including a packet gateway node (PGN) with an internet connection, the PGN being capable of acting as a mobile IP home agent (HA) with authentication of a MN handled by the GPRS/UMTS network before the PGN ever sees data traffic to establish a Mobile IP authentication key, wherein an unauthenticated key exchange method such as Diffie-Hellman, the MVQ protocol or its one-pass variant (without certificates), or the Key Exchange Algorithm can be used to establish the shared key.

14. A system according to claim 10, wherein in addition, the initial key forms the basis for subsequent key exchanges using a standard's based protocol.

15. A system according to claim 14, wherein the standard's based protocol is IPsec.

16. A system according to claim 15, wherein with a shared key in place, the Mobile IP authentication key is derived by performing an MD-5 hash of the shared key whereby pre-programming of the authentication key is not needed and the authentication key need not remain static.

17. A system according to claim 16, wherein subsequent traffic between the MN and the PGN is encrypted using an authenticated key exchange with the IKE aggressive mode key exchange (very fast) using the shared key to establish a large encryption key and an SA.

18. A system according to claim 17, further comprising:

a wireless local area network (WLAN) with a wireless access node and an internet connection;

a connection between the MN and the WLAN;

a Mobile IP care-of-address obtained from a DHCP server through the connection between the MN and the WLAN.

19. A system according to claim 18, wherein said authentication value is a 128 bit authentication value.